

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*THE513BLACKJEEP@GMAIL.COM THAT IS STORED AT
PREMISES OWNED BY GOOGLE INC.Case No. **1:19-MJ-00796**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-4

located in the _____ Southern _____ District of _____ Ohio _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

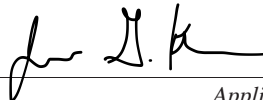
18 U.S.C. § 2252/2252A

POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

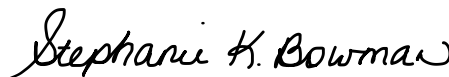
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

SPECIAL AGENT JASON G. KEARNS, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: **Nov 21, 2019***Judge's signature*City and state: **CINCINNATI, OHIO**

HONORABLE STEPHANIE K. BOWMAN

Printed name and title

ATTACHMENT A-4

Property to Be Searched

This warrant applies to information associated with **THE513BLACKJEEP@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Way, Mountain View, California.

ATTACHMENT B-4

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on February 13, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-4:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.
- g. Notwithstanding Title 18, United States Code, Section 2252A, Google may disclose responsive data, if any, by delivering encrypted files through Google’s Law Enforcement Request System (LERS).

II. Information to be seized by the government

- a. All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography; violations of U.S.C. § 2252A(a)(2), which makes it a crime to distribute or receive child pornography in interstate commerce by computer including the following:
1. Communications about or reflecting the transportation, possession, receipt, distribution, or production of child pornography;
 2. Communications that reveal, or provide leads to identify the account owner and additional co-conspirators;
 3. Documents, photographs, digital files, or other electronic media, attached or otherwise stored electronically, related to any of the above-listed matters.
 4. Any child pornography or child erotica; and
 5. Any information concerning or relating to Bitcoin or the use of bitcoin.

Pursuant to 18 U.S.C. §§ 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

Pursuant to 18 U.S.C. §§ 2256(1), the term “minor,” as “any person under the age of eighteen.”

- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jason G. Kearns a Special Agent (“SA”) with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”) since 2005 and am currently assigned to Cincinnati. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have also participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252/2252A (Possession, Receipt, & Distribution of Child Pornography) have been committed by Bryan Lamont Johnson (DOB XX/XX/1990). This Affidavit is submitted in support of Applications for search warrants for the following:

- a. The Apple iTunes/iCloud account **BRYANJOHNSON513@GMAIL.COM**; as more fully described in Attachment A-1. The items to be searched for and seized are described more particularly in Attachment B-1.
- b. The Apple iTunes/iCloud account **THE513BLACKJEEP@GMAIL.COM**; as more fully described in Attachment A-2. The items to be searched for and seized are described more particularly in Attachment B-2.
- c. The Google account **BRYANJOHNSON513@GMAIL.COM**; as more fully described in Attachment A-3. The items to be searched for and seized are described more particularly in Attachment B-3.
- d. The Google account **THE513BLACKJEEP@GMAIL.COM**; as more fully described in Attachment A-4. The items to be searched for and seized are described more particularly in Attachment B-4.
- e. The Dropbox account **GO513HARD@GMAIL.COM**; as more fully described in Attachment A-5. The items to be searched for and seized are described more particularly in Attachment B-5.

Upon receipt of the information described in Section I of the respective Attachment B (1-5), government-authorized persons will review that information to locate the items described in Section II of the respective Attachment B (1-5).

3. The statements in this affidavit are based on my investigation of this matter as well as information conveyed to me by other law enforcement officers, to include other HSI agents as well as special agents of the United States Internal Revenue Service, Criminal Investigation (“IRS-CI”). Since this affidavit is being submitted for the limited purpose of

securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution and receipt of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct).

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has

been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet service providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the

Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

q. Whois: A “Whois” search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0– 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0– 12.345.67.99.

BACKGROUND ON TOR AND BITCOIN

7. Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering conventional Internet Protocol ("IP") address-based methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle," which is available at www.torproject.org.¹ When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, appears on the website's IP address log. Currently, there is no practical method to trace a user's actual IP address back through those Tor relay computers.

8. The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Like other websites, "hidden services" are hosted on computer servers that communicate through IP addresses. However, hidden services bear some unique technical features that conceal the computer server's location. As distinguished from standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, such as "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, it is possible for investigators to determine the IP address of the computer server hosting a website through a simple public lookup via a Domain Name System ("DNS") listing. Unlike ordinary Internet websites, there is no publicly available query that may be performed via a DNS listing to

¹ Additional information outlining Tor and how it works is publicly accessible at www.torproject.org.

determine the IP address of the computer server that hosts a Tor hidden service. Although law enforcement agents may be able to view and access hidden services that are facilitating illegal activity, the IP address of a Tor hidden service cannot be determined via public lookups.

Moreover, communications between users' computers and a Tor hidden service web server are routed – as with all Tor communications – through a series of intermediary computers.

Accordingly, neither law enforcement nor hidden service users can determine the true IP address – and therefore the location – of the computer server that hosts a hidden service through public lookups or ordinary investigative means.

9. Bitcoin (“BTC”) is a type of virtual currency, circulated over the internet.² BTC are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. BTC is just one of many varieties of virtual currency.

10. BTC are sent to and received from BTC “addresses.” A BTC address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each BTC address is controlled through the use of a unique corresponding private key – which is a cryptographic equivalent of a password or pin needed to access the address. Only the holder of an address' private key can authorize any transfers of BTC from that address to other BTC addresses. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for each and

² Since BTC is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

every transaction.

11. To acquire BTC, a typical user will purchase them from a BTC virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information of their customers and verify their clients' identities.

12. To transfer BTC to another address, the sender transmits a transaction announcement, which is cryptographically signed with the sender's private key, across the peer-to-peer BTC network. The BTC address of the receiving party (who has a private key) and the sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain – which is decentralized public ledger that records all BTC transactions. The blockchain logs every BTC address that has ever received a BTC and maintains records of every transaction for each BTC address.

13. While the identity of a BTC address owner is generally anonymous (unless the owner opts to make information about the owner's BTC address publicly available), analysis of the blockchain can often be used to identify the owner of a particular BTC address. Since the

blockchain serves as a searchable public ledger of every BTC transaction, investigators may trace transactions to BTC exchangers. Because those exchangers generally collect identifying information about their customers, subpoenas or other appropriate process submitted to these exchangers can, in some instances, reveal the true identity of an individual responsible for a BTC transaction.

14. Analysis of the blockchain can also, in some instances, reveal whether additional BTC addresses are controlled by the same individual or entity. For example, the proprietor of a website that accepts payment via BTC may create many BTC addresses in order to receive payments from different customers. If the proprietor decides to consolidate the BTC that it has received from those customers, the proprietor may group those many BTC addresses together in order to send a single transaction into one BTC account. Each of those many BTC addresses would then appear as “inputs” on a single transaction on the blockchain. Examining the transactions associated with a known BTC address may therefore reveal the existence of other BTC addresses that appeared as “inputs” alongside the known address – which indicates that the addresses were controlled by the same user. Additional examination of those BTC addresses and their activity on the blockchain may reveal further information about the user and his/her previous transactions.

15. Law enforcement uses sophisticated commercial services offered by several different blockchain analysis companies to investigate bitcoin transactions. These companies analyze the blockchain in an attempt to identify individuals or groups involved with bitcoin transactions. Specifically, these companies create large databases that group bitcoin transactions into “clusters” through analysis of data underlying bitcoin transactions. The service allows law

enforcement to identify BTC addresses that are included as “inputs” in the same transaction, as described above, and “cluster” these addresses together. Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable.

16. This third-party blockchain analysis software is an anti-money laundering software used by banks and law enforcement organizations worldwide. It has supported many investigations, and been the basis for numerous search and seizure warrants. As such, law enforcement has found the information provided by it to be reliable. Further, computer scientists have independently shown that they can use “clustering” methods to analyze clues in how bitcoins are typically aggregated or split up to identify BTC addresses and their respective account owners. As described below, the “clustering” analysis conducted in this investigation has been corroborated through numerous search and arrest warrants which have uniformly found connections to child exploitation and child pornography for the BTC addresses in question.

THE WEBSITE

17. “The Website”³ is a website dedicated to the advertisement and distribution of child pornography that operates as a hidden service on the Tor network. As of September 28, 2017, and again on February 8, 2018 and February 22, 2018, law enforcement agents accessed The Website and documented its content, as described herein. The Website is used to host and distribute image and video files depicting child pornography and child erotica that may be downloaded by site users. While there may be some images depicting adult pornography accessible on The Website, the overwhelming majority of images and videos observed by law enforcement agents appear to be child pornography or child erotica. In fact, the upload page on The Website clearly states: “Do not upload adult porn.”

18. Any user may create a free account on The Website by providing a username and password. Only after the user has registered an account, can the user browse previews of videos that are available for download and post text to The Website. In order to download videos from the site, however, the user must use “points,” which are allocated to users by The Website. A registered user can earn points by: (1) uploading videos depicting the sexual exploitation of children; (2) referring new users to The Website; (3) paying for a “VIP” account, which lasts for six months, entitles a user to unlimited downloads, and is priced at 0.03 BTC (approximately

³ The actual name of “The Website” is known to law enforcement. The Website remains active and disclosure of the name of The Website would potentially alert its users to the fact that law enforcement action is being taken against users of The Website, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified herein as “The Website.”

\$327.60 as of March 1, 2018); or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points).⁴

19. During the course of the investigation, law enforcement agents accessed The Website on multiple occasions and also conducted an undercover purchase of VIP access to The Website. Based on review of that activity, it appears that the Website assigns each user who accesses the site a unique BTC address to which the user can send funds for purchasing account privileges.

20. Each video available for download has a title, a description (if added by the uploader), “tags” with further descriptions of the video which enable a user to more easily locate a particular category of video using The Website’s search function, and a preview thumbnail image that contains approximately 16 unique still images from the video. As of February 8, 2018, The Website had over 125,000 unique videos available for downloading. In order to prevent duplicate videos from being uploaded, The Website provides a digital hash-value check in order for the user to compare his or her video to other videos previously uploaded to the site.⁵ The Website does not allow a user to upload a video whose hash value matches one that had previously been uploaded to the site. According to law enforcement’s viewing of The Website as of February 8, 2018, the videos stored on The Website amount to over seven terabytes of data. As a point of comparison, seven terabytes of data would fill roughly 10,486 CD-ROM discs. As

⁴ Bitcoin is volatile and the price of bitcoin can fluctuate on an hourly basis. Between January 2017 and February 2018, for example, 1 bitcoin has fluctuated in price from approximately \$1,000 to \$20,000 USD. As of February 13, 2018, 1 bitcoin is worth approximately \$8,600.

⁵ A hash value refers to a unique value calculated for a particular file or set of files, sometimes referred to as a digital fingerprint.

of February 8, 2018, The Website indicated on its download page details that its users have downloaded files on The Website more than one million times.

21. Examples of video files on The Website that have been downloaded by law enforcement agents include one that is approximately ten minutes long. Law enforcement reviewed the preview stills of the video. The video depicts a prepubescent Asian girl who appears, from her small stature, lack of breast development, and absence of pubic hair, to be approximately nine to eleven years old. The child is naked with her hands duct-taped to her ankles on either side. A naked adult male is vaginally penetrating the child's vagina while simultaneously inserting multiple object into the child's vagina. It appears that this video was uploaded by the site's administrator.

22. Another downloaded video on the site is approximately eight-and-a-half minutes long. A user uploaded the video to the site with the description of "8yo anal fucked pussy". Law enforcement reviewed the preview stills of the video. The video depicts a prepubescent girl who appears, from her small stature, youthful appearance, and lack of breast development or pubic hair, to be between the ages of six and eight years old. The child's underwear is are pulled down around her thighs and the child is positioned on all fours while a naked adult male penetrates the child's vagina with his penis from behind. The adult male repositions the child and then moves the child in several different positions while continuing to penetrate her vagina with his penis.

23. Other examples of videos from The Website include depictions of toddlers and infants engaged in sexually explicit conduct. For example, law enforcement reviewed still images from a video that is approximately one minute and twenty-three seconds long, which

depicts a toddler girl who appears to be between the ages of approximately two and three years old. The video shows the child being anally penetrated by an adult male while she cries into her hands. The video zooms in to focus on the toddler's vaginal area as the adult male penis penetrates the toddler's anus.

24. Your affiant also reviewed the still images of a video that is approximately thirty-three minutes and forty-four seconds long, which depicts a baby approximately six months old who is holding an adult penis. In another still frame, the adult male is holding his penis and inserting his penis into the baby's mouth. In the last still frames, the adult male is forcing his penis into the baby's anus. The images and videos discussed above are representative, but by no means exhaustive, examples of the types of videos available for download on The Website.

25. On the video search page of The Website, there is a list of keyword search terms and the number of videos associated with the keyword. As of February 8, 2018, some of the top keyword search terms included "PTHC" (over 10,000 videos), "PEDO" (over 7,000 videos), "2yo%" (over 4,000 videos) and "%4yo" (over 4,000 videos).⁶

Identification and reliability of The Website "cluster"

26. As described herein, based on investigation to date, The Website appears to assign each user who accesses the site a unique BTC address to which the user can send funds for purchasing account privileges. Based on prior investigations, law enforcement is aware that creating such a payment system allows the reliable third-party blockchain analysis software to group the payments together into a cluster associated with the recipient.

⁶ I am aware from training and experience that "PTHC" stands for "preteen hardcore," PEDO is a reference to "pedophile," and the references to "2yo" and "4yo" represent ages of children.

27. The third party who operates this software proactively seeks out sites on the Tor network and related clusters engaged in illicit activity, in part so that institutions that are required to perform due diligence can ensure that they are not sending funds to illicit sites.

28. In fact, while conducting such due diligence analysis, the reliable third-party blockchain analysis software clustered thousands of BTC addresses together that the software concluded to be associated with The Website (“The Website Cluster”). After the reliable third-party blockchain analysis software identified The Website Cluster, it marked the cluster as being associated with child pornography.

29. The third-party blockchain software revealed that from approximately October 2015 to approximately February 8, 2018, The Website Cluster has received approximately 411 BTC worth \$324,961 at the time of transaction.⁷

30. IRS-CI independently corroborated this “clustering” analysis by following a controlled payment of BTC from an undercover agent’s BTC wallet to a unique BTC address provided by The Website. Within one day of this undercover payment, the reliable third-party blockchain analysis software independently added the unique receiving BTC address to The Website’s cluster. A subsequent analysis of the blockchain revealed that The Website Cluster cashed out this undercover payment and numerous other payments in the cluster into a BTC wallet held in the name of the suspected administrator (who is described further below).

31. To further the investigation and further corroborate The Website Cluster, law

⁷ To date, the investigation has not found evidence that The Website Cluster is associated with any other website or web services, although it is technically possible that individual BTC transactions made to BTC addresses within The Website Cluster could be unrelated to The Website.

enforcement issued subpoenas to the virtual currency exchanges that had customers who sent BTC directly to The Website Cluster. Virtual currency exchanges, which act as financial institutions, maintain due diligence records related to their customers. Subpoena returns from one such virtual currency exchange yielded records for numerous accounts registered there that sent BTC to The Website Cluster. The subpoena returns revealed customer names as well as additional identifiable information. Many of the customers reside in the United States. Of the numerous accounts discovered in the returns, approximately 22 had sent BTC to The Website with a note connected to the transaction listing what appears to be a username on The Website or other information further connecting the transaction to The Website (*e.g.*, “[The Website] VIP” and “for User: [username] (230 downloads)”).

32. The subpoena returns specifically identified two customers whose BTC addresses were observed on the blockchain to have transacted with BTC addresses within The Website Cluster and also contained two apparent usernames. By using the search-by-uploader function on The Website, IRS-CI determined that the two usernames listed in the transaction notes of BTC sent to The Website matched the usernames of two accounts that uploaded child pornography videos to The Website.

33. Subsequent judicially authorized search warrants for customers identified by The Website Cluster, for whom virtual currency exchanges had personal identification information, has further corroborated the reliability of the software. As of March 9, 2018, each search warrant of such customer’s residence has yielded evidence of child exploitation and/or child pornography relating to the customer.

Investigation of the suspected administrator of The Website

34. Your affiant is aware that typically Tor network site administrators are typically the only people able to access and transact in the revenue generated by their websites. Thus, as part of the investigation of The Website, law enforcement began following the BTC transactions going out from The Website Cluster in an attempt to locate the administrator of the site. Law enforcement has repeatedly found that this practice of “following the money” to be an effective way of learning who is profiting from a criminal enterprise, and is thus responsible for the criminal activity.

35. Utilizing the reliable third-party blockchain analysis software and documents produced by numerous virtual currency exchanges, law enforcement was able to trace the BTC sent out by The Website Cluster to several BTC accounts held in the names of the suspected administrator and his father. These BTC accounts ultimately cashed out into bank accounts again held in the names of the suspected administrator and his father.

36. On or about September 1, 2017, law enforcement reviewed the source code of The Website’s homepage, which can be viewed by right-clicking on The Website in the Tor browser and selecting “View Page Source.” In reviewing the source code, law enforcement discovered that The Website had failed to conceal an IP address, likely due to user error on the part of the administrator. This IP address resolved to a telecommunications provider in South Korea. Subsequent investigation confirmed that this IP address was registered in the name of the suspected administrator and was serviced at the suspected administrator’s residence.

37. On February 28, 2018, a federal magistrate judge in the United States District Court for the District of Columbia issued an arrest warrant for the suspected administrator.

38. On or about March 5, 2018, foreign law enforcement executed a search warrant of

the residence of the suspected administrator and his father. Pursuant to the search, foreign law enforcement seized The Website's server and associated electronic storage media from the bedroom of the suspected administrator. Foreign law enforcement then provided a forensic image of this media to U.S. law enforcement, for which U.S. law enforcement obtained a search warrant to review.

39. The search warrant returns of the imaged media revealed over 120,000 videos hosted on The Website as well as customer data. A review of a sample of these video further corroborated that The Website appears to be entirely dedicated to child pornography. The customer data generally identified which user was associated with which BTC payment to The Website, and confirmed that such users downloaded content from The Website. A review of a sample of the payments to The Website Cluster cross-referenced against the user id and download data from the server revealed that each payment to The Website Cluster resulted in the user downloading at least one video from The Website.

PROBABLE CAUSE

40. Based on the instant investigation as described further herein, there is probable cause to believe that Bryan Lamont Johnson associated with 5206 Ravenna Street, Cincinnati OH 45227 has engaged in BTC transactions with BTC addresses within The Website Cluster, in amounts that appear to be consistent with payments for "points" on The Website.

41. The response to a subpoena to U.S. BTC Exchange revealed a BTC account 5a2732c9334f0701087833b1 created on December 5, 2017 that included the following

associated identifiers⁸:

Name: Bryan Johnson

Email: bryanjohnson513@gmail.com

SSN: XXXXX9487

Address: 5206 Ravenna Street, Cincinnati OH 45227

DOB: X/XX/1990

Phone Number: 5134985342 (verified)

Billing Address: 5206 Ravenna Street, Cincinnati OH 45227

Bank Account (verified)

Customer Name: Bryan Lamont Johnson

Bank Name: Chase – Total Checking

Account Number: XXXXX5930

Routing Number: XXXXX037

Payment Cards (verified)

Customer Name: Bryan Johnson

Last 4 Digits: XXXXXX****7965

Expiration Month: 11

Expiration Year: 2020

Issue Type: Visa Debit

Issuer: JP Morgan

⁸ Portions of identifying information have been redacted by placing a “X” in their place to comport with the court’s cm/ecf filing requirements.

As noted above, the phone number, email account, bank account, payment account were all verified to be active and valid.

42. Between December 5, 2017 and February 25, 2018 the BTC account 5a2732c9334f0701087833b1 engaged in four transactions with BTC addresses within The Website Cluster. The first transaction occurred on or about December 5, 2017 for approximately 0.03947634 BTC.

43. The second transaction occurred on December 26, 2017 for approximately 0.0002869 BTC. The third transaction occurred on January 14, 2018 for approximately 0.00013365 BTC, and the final transaction occurred February 25, 2018 for approximately 0.00310728 BTC.

44. There were two usernames associated with these transactions. The first username was "jeep513". "jeep513" downloaded approximately 20 videos on or about January 14 and 15, 2018. One of the videos was titled "Pedo (Pthc) - 2 8Yo Mexicans Preteens With Male (Hussyfan) (r@ygold) (babyshivid) - music! sound.mpg". The video is approximately 51 minutes and 57 seconds. The video starts off with a prepubescent female performing oral sex on a dildo. The prepubescent female then performs oral sex on an adult male. Later on the video, the adult male has vaginal intercourse with the prepubescent female.

45. The second username was "jeep4545". "jeep4545" downloaded approximately 34 videos on or about February 26 and 27, 2018. One of the videos was titled "real hardcore gitl 8yo fuck pussy anal rape extreme fuck.avi". The video is approximately 6 minutes and 20 seconds long. The video shows an adult male having sex with a prepubescent female.

46. A check of the CLEAR (Consolidated Lead Evaluation and Reporting) informational database, on or about September 24, 2019, revealed that Bryan Johnson resides at the 5206 Ravenna Street, Cincinnati OH 45227. CLEAR is a public record data investigative platform available exclusively to law enforcement and other government investigators about people and businesses.

47. A check with the Department of Motor Vehicles, on or about September 24, 2019, revealed that an individual named Bryan L. Johnson with a date of birth of September 10, 1990 and social security number of 283929487 resides at the 5206 Ravenna Street, Cincinnati OH 45227. The check also revealed that Johnson had a 2016 black Jeep wrangler registered in his name at the 5206 Ravenna Street, Cincinnati OH 45227.

48. On or about September 24, 2019, a check of the Hamilton County Auditors website indicated that Bryan Johnson was the owner of the 5206 Ravenna Street, Cincinnati OH 45227.

49. Surveillance of the 5206 Ravenna Street, Cincinnati OH 45227 on or about on or about September 23, 2019 revealed that a black Jeep wrangler was parked in the driveway of the 5206 Ravenna Street, Cincinnati OH 45227.

50. A search of Accurant information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for Johnson. These public records indicated that Johnson's current address is the 5206 Ravenna Street, Cincinnati OH 45227. Accurant also indicated that the email accounts bryanJohnson513@gmail.com and MY513JEEP@gmail.com were associated with Johnson.

51. On October 9, 2019, HSI Cincinnati executed a federal search warrant at 5206 Ravenna Street, Cincinnati OH 45227. Bryan Lamont Johnson was home at his residence. Johnson was advised HSI had a search warrant for the residence. The affiant and SA Cameron Bryant advised Johnson that he was not under arrest and asked if he would be willing to talk. Johnson agreed and Johnson was provided some clothes to put on. Johnson followed the affiant and SA Bryant to the affiants' vehicle parked outside of his residence, 5206 Ravenna St., Cincinnati OH 45227.

52. The affiant advised Johnson that he was not under arrest and that he was free to leave at any time. The affiant then read Johnson the Miranda warnings which Johnson stated that he understood. Johnson then read the Miranda warnings which he signed and waived his rights to an attorney.

53. Johnson advised that he has lived at 5206 Ravenna St. in Cincinnati for approximately three years and that his name is on the house. Johnson provided his phone of 513-780-7338. He advised that it was his cell phone number which is though T-Mobile. He is currently unemployed and collecting unemployment. Johnson previously worked at Coca-Cola on Red Bank Road in the warehouse. Cincinnati Bell / Fioptics is his current internet service provider. Johnson stated that his current/main email address that he utilized was bryanjohnson513@gmail.com. Johnson indicated that his internet usage consists looking at sports, play video games, and streaming movies, which included movies that were currently in the theaters. Johnson said that he had heard of TOR (The Onion Router). Johnson advised that he currently did not have a computer in his residence. He stated that he had come into some "hard times" and had to pawn his computer. Johnson advised that he had an iPhone 11 that he

just got as an upgrade from his previous iPhone but had no idea where it was located in the residence. Johnson advised that the only electronics that he has was his iPhone, router, Xbox, and Apple TV. Johnson then advised that he researches bitcoins and TOR on the internet. Johnson then denied purchasing bitcoins or any cryptocurrency.

54. Johnson stated that he used to bank with Chase and previously had a JP Morgan debit card. He got rid of them. Johnson also stated that he used to have the phone number 513-498-5342. The affiant advised that all his “old” banking information, old phone number and current email address were tied to the purchase of cryptocurrency. Johnson then provided the password “091090” for his iPhone and stated that it was probably on his nightstand in his bedroom. Johnson said that he sold his MacBook. Johnson advised that the email account bryanjohnson513@gmail.com is his iCloud account. A review of Johnson’s cell phone indicated he had an iTunes account with the email account bryanjohnson513@gmail.com and that he had a second iTunes account. The email the513blackjeep@gmail.com was associated with the second iTunes account and accessed on or about October 6, 2019. Johnson then advised that he bought something off of the internet using cryptocurrency and maybe used it once or twice. Johnson indicated that his Chase bank account was terminated by the bank because of too many overdraft fees. Johnson said that he could not remember what he purchased with the cryptocurrency.

55. Johnson advised that he keeps to himself, and that he has not been in a relationship with a woman for a while. Johnson said that he looks at pornography on sites like X videos and Pornhub. He looks for interracial, porn star, role playing, two girls, “all straight”. Johnson advised that it is possible that he ended up on sites like “barely legal” or sites like that. Johnson said that he understood that sex involving anyone under the age of 18 is considered

child pornography. Johnson then advised that he used to have an iMac computer as well but got rid of it.

56. Johnson was asked if he had a TOR browser app. Johnson said that he did not know because he had so many apps on his phone. Johnson then stated he may have used it a few times in the past but not in the last few days. Johnson said through his research that you can buy guns or drugs using the TOR browser.

57. Johnson advised that his previous iPhone was an iPhone 10 and he had it for approximately two years. He paid approximately \$300 for the upgrade to the new iPhone.

58. Johnson advised that he utilizes Dropbox but was not sure what email account was associated with the Dropbox account. A review of Johnson's cell phone indicated that the email address go513hard@gmail.com was the email account signed into his Dropbox account. The account was accessed on or about October 5, 2019. Johnson advised that he has had the account for approximately five years. Johnson advised that he also uses Drive (One Drive) for cloud-based storage.

59. Johnson indicated that he has never utilized his Xbox for accessing the internet other than one time to do an internet speed test.

60. Johnson said that had Firefox as a backup top look at websites that don't work well in Safari. Johnson indicated that he did not have Google Chrome. Johnson also said that he did not have any thumb drives or memory cards.

61. Johnson advised that he purchased the iPod approximately three years ago off of Craigslist three years ago and met the person selling it at Walmart. Johnson admitted to watching bondage videos. Johnson said that when his old cell phone was broken, he utilized the

iPod to look at pornography. Johnson advised that he was willing to go to counseling if this will resolve the issue. Johnson said that if there was child pornography on his device then it was an accident. He said that if he had seen it, he would have thrown it away. Johnson advised that he looks at a lot of porn and maybe he just “Googled it”. Johnson then advised that he may have accidentally viewed a child pornography website. There was a girl on the website that may have been 16 or 17 years old. Johnson could not remember connecting his iTunes account to his iPod.

62. Johnson advised that he could not remember what he purchased with his cryptocurrency.

63. Johnson also advised that the memory card located in his residence was still in the package and had never been used. A review of the memory indicated that the memory card contained the backup of a cellular telephone.

64. There were several recent searches on Johnson’s cell phone of how to clear safari cache, creating a new iTunes account and signing out of an iTunes account. At the time of the writing of this affidavit, forensics is still being conducted on the items seized from Johnson’s residence.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

65. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers

basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of

images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person.

Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example,

“bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

INFORMATION REGARDING APPLE ID AND iCloud⁹

66. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

67. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

⁹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

68. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

69. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user

accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

70. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

71. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service,

including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

72. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

73. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain).

iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

74. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

75. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

76. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

77. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

78. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND CONCERNING EMAIL

79. In my training and experience, I have learned that Google, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, Inc. allows subscribers to obtain email accounts at the domain name Gmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, Inc. subscribers) and information

concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

80. A Google subscriber can also store with the provider files in addition to emails such as pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, Inc.

81. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

82. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the

account. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

83. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

84. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained

by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

BACKGROUND CONCERN DROPBOX

85. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at <https://www.dropbox.com/privacy>, Dropbox collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system

configuration information, metadata concerning your Files, and other interactions with the Service. “Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website.”

86. The Dropbox Law Enforcement Handbook also states that Dropbox maintains IP addresses for web-based logins and the last-seen IP address of linked computers. IP address information is typically maintained for 6 months, but this may be extended with a preservation request. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available. IP address login information is recorded when a user logs in to Dropbox through the website. Like many online services, Dropbox sometimes uses cookies stored on a browser so that a user may not need to sign in every time they visit the website. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox.

87. In general, providers like Dropbox ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the

account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. Additionally, providers like Dropbox commonly keep records about whether the email address used to create the account was verified. The verification of the email address associated with the account can occur several ways, one is by sending an email to the address asking the account user to confirm it created the dropbox account.

88. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE, POSSESS,
AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY**

89. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess, and/or access with intent to view child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are

often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹⁰

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography

¹⁰ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Johnson uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home.

90. Based on the following, I believe that Bryan Lamont Johnson residing at 5206 Ravenna Street, Cincinnati OH 45227 likely displays characteristics common to individuals who receive, possess or access with intent to view child pornography.


91. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrant will be served on Dropbox.com, Google, and Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING OF AFFIDAVIT

92. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

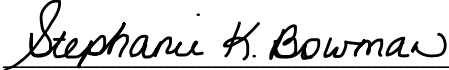
CONCLUSION

93. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachments B1 – B5, are located at the locations described in Attachments A1 – A5. I respectfully request that this Court issue a search warrant for the locations described in Attachment A1-A5, authorizing the seizure and search of the items described in Attachment B1 – B5.



Jason G. Kearns
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 21th day of November, 2019.



UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A-4

Property to Be Searched

This warrant applies to information associated with **THE513BLACKJEEP@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Way, Mountain View, California.

ATTACHMENT B-4

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on February 13, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-4:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.
- g. Notwithstanding Title 18, United States Code, Section 2252A, Google may disclose responsive data, if any, by delivering encrypted files through Google’s Law Enforcement Request System (LERS).

II. Information to be seized by the government

a. All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography; violations of U.S.C. § 2252A(a)(2), which makes it a crime to distribute or receive child pornography in interstate commerce by computer including the following:

1. Communications about or reflecting the transportation, possession, receipt, distribution, or production of child pornography;
2. Communications that reveal, or provide leads to identify the account owner and additional co-conspirators;
3. Documents, photographs, digital files, or other electronic media, attached or otherwise stored electronically, related to any of the above-listed matters.
4. Any child pornography or child erotica; and
5. Any information concerning or relating to Bitcoin or the use of bitcoin.

Pursuant to 18 U.S.C. §§ 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

Pursuant to 18 U.S.C. §§ 2256(1), the term “minor,” as “any person under the age of eighteen.”

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.